Configuring Protocol-Independent Match Conditions

Table 1 describes the firewall filter match conditions for protocol-independent traffic.

To configure firewall filter match conditions for protocol-independent traffic:

- Include the *match-conditions* statement at the [edit firewall family any filter *filter-name* term *term-name* from] hierarchy level.

Table 1: Protocol-Independent Firewall Filter Match Conditions

Match Condition	Description
forwarding-class *class*	Forwarding class. Specify assured-forwarding, best-effort, expedited-forwarding, or network-control.
forwarding-class-except *class*	Do not match on the forwarding class. Specify assured-forwarding, best-effort, expedited-forwarding, or network-control.
interface *interface-name*	Interface on which the packet was received. You can configure a match condition that matches packets based on the interface on which they were received.
interface-set *interface-set-name*	(MX Series routers and routers with Enhanced IQ2 [IQ2E] PICs only) Interface set on which the packet was received. An interface set is a set of logical interfaces used to configure hierarchical class of service schedulers. For information about configuring an interface set, see the *JUNOS Class of Service Configuration Guide* and the *JUNOS Network Interfaces Configuration Guide*.
packet-length *bytes*	Length of the received packet, in bytes. The length refers only to the IP packet, including the packet header, and does not include any Layer 2 encapsulation overhead.
packet-length-except *bytes*	Do not match on the received packet length, in bytes.

Published: 2010-04-15